Volume 17, Issue 04   Atari Online News, Etc.   January 23, 2015

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1704   01/23/15

~ Big Brother in Schools? ~ Lizard Squad Is Hacked! ~ Google Glass Future

-* China Blocks Some VPN Services *-
-* "Self-aware" Super Mario Is Created *-
-* U.S. Penetrated N. Korea Networks Years Ago -

=~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Well, we're here getting ready for the first "real" Nor'easter of the season this weekend. I'm not looking forward to clearing snow, but that's the reality of living in New England (and other areas of "snow country"). But, I don't have to like it!

It's been a long and stressful week, but I'm hoping that over the next few weeks, things may finally start to get back to normal.

Speaking of normal, let's get right to this week's issue!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Goodbye to Club Nintendo Loyalty Rewards Program!
""""""""""""""""""""""""""""""   Researchers Create 'Self-aware' Super Mario!

'Resident Evil 7' Release Date!
And more!

=~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Say Goodbye to Club Nintendo Loyalty Rewards Program

If you happen to be a member of Club Nintendo, then it's time to go clear out your Coin balance.

Nintendo on Tuesday announced plans to shut down the loyalty rewards program after more than six years. Members earned Coins by doing things like registering products and completing surveys, which they could spend on rewards like downloadable games, Nintendo posters, and character figures.

Nintendo didn’t specify why it’s shutting down the program, but the company apparently has something new in the works, as it promised to launch a new loyalty program "at a later date."

As The Verge points out, Club Nintendo was never a huge success in the U.S. or Europe. It’s a different story in Japan, however, where members could nab perks like limited-edition games and handhelds. The program is shutting down globally, so we’re sorry to pass along this news if you’re a happy member.

"We thank all Club Nintendo members for their dedication to Nintendo games and their ongoing love for our systems and characters," Scott Moffitt, Nintendo of America’s executive vice president of sales and marketing, said in a statement. "We want to make this time of transition as easy as possible for our loyal Club Nintendo members, so we are going to add dozens of new rewards and downloadable games to help members clear out their Coin balances."

You can still sign up for the program and earn Coins through the end of March, and redeem prizes through June. Nintendo promised to add a number of physical reward options and downloadable games for members to choose from next month.

As a peace offering, Nintendo is planning to offer the Flipnote Studio 3D software to members for free in February. The software lets you create 3D animations and exchange your creations with others. Anyone who creates a Club Nintendo account before registration closes on March 31 will be eligible to receive this software.

Researchers Create ’Self-aware’ Super Mario with Artificial Intelligence

A team of German researchers has used artificial intelligence to create a "self-aware" version of Super Mario who can respond to verbal commands and automatically play his own game.

The Mario Lives project was created by a team of researchers out of Germany’s University of Tübingen as part of the Association for the Advancement of Artificial Intelligence’s (AAAI) annual video competition. Each year the competition showcases videos from researchers and scientists from around the world that demonstrate "exciting artificial intelligence advances in research, education, and application."

The video depicts Mario’s newfound ability to learn from his surroundings and experiences, respond to questions in English and German and automatically react to "feelings."

If Mario is hungry, for example, he collects coins. "When he’s curious he will explore his environment and autonomously gather knowledge about items he doesn’t know much about," the video’s narrator explains.

The video also demonstrates Mario’s ability to learn from experience. When asked "What do you know about Goomba"   that’s Mario’s longtime enemy in the Super Mario series   Mario first responds "I do not know anything about it."

But after Mario, responding to a voice command, jumps on Goomba and kills it, he is asked the question again. This time, he responds "If I jump on Goomba then it maybe dies."

The team behind Mario Lives, from the University of Tübingen’s Cognitive Modeling department, used Carnegie Mellon’s speech recognition software and principles of psychology to create the new "self-aware" version of Nintendo’s famous plumber, according to the video.

’Resident Evil 7’ Release Date, Gameplay & Trailer: Better Than ’Resident Evil 6’?

Will the next "Resident Evil" installment outshine its predecessor? According to the January 19 report of Master Herald, there is a high possibility that the upcoming "Resident Evil 7" game will be better than the "Resident Evil 6."

Since the "Resident Evil" franchise is known for its continuously good reviews and exceptional high quality of action and horror, it is therefore expected that this trend continues in the next installments to come. "The new game is going to push the boundaries of how some people perceive horror, and will include surprises that some fans might find downright disturbing," says Master Herald’s Arash Fekri.

With these new advancement in gaming technology, the next "Resident Evil 7" is not only expected to get new game story and game play, but it is also expected have better graphics, sounds, and physical appearance.

Master Herald notes that the new "Resident Evil" game has a lot of potential because developers have more time and more resources to use to experiment and make the game even better and more horrifying than it has delivered over the years. The news outlet also revealed a leaked screenshot of the game which can attest to the "spectacular and significantly better" "Resident Evil 7" game. Check out the screenshot here.

Meanwhile, Capcom producer Michiteru Okabe earlier revealed how they are developing the new game based on the comments from fans. "I think one thing that’s become really clear is that people want out of the Resident Evil series is survival horror first and foremost...They want that to be the core of the gameplay. I think what we really need to do is take a serious look at what makes the series itself. Look at all the constituent parts-if resource management is important to survival horror, then why is it important, what does it mean, and what do these varying elements mean to the franchise? and How can we then take that and work with modern technology?" Okabe was quoted as saying by the Express.

Okabe further said that they are indeed experimenting and trying "bold, new things" and continuing refining ideas that have already left a mark to the fans. "I think the big numbered titles are where we try the big sort of experiments...We see what sticks, and continue to refine those ideas...I think with the spin-off series we have the opportunity to do something a little different," to quote him.

The rumors about the "Resident Evil 7" game being developed started in 2013 when Game Spot reported that an unnamed ex-employee of the motion capture studio House of Moves revealed that a new "Resident Evil" game is already on the works. The unnamed employee claimed on LinkedIn that she worked as a "costume designer for the video game Resident Evil 7" from November 2012 to January 2013.

The release date of the "Resident Evil 7" game is still unknown.

New NASCAR Game Underway for PS4, Xbox One, and PC

A NASCAR game for PlayStation 4, Xbox One and PC is in development at a newly announced studio, DMi Games.

As of January 1, the North Carolina-based DMi Games had acquired the license to develop and publish games in the series from previous custodian Eutechnyx. The change in ownership was said to be complex due to the complexity of the licence agreements.

DMi Games president Ed Martin explains: "Just to give you some context, a contemporary NASCAR video game has more than 1,000 licensed and approved properties in it. That s a lot of stakeholders and people to get organized!"

Martin, who has been working on NASCAR games since the early ’90s, announced the new deal in an open letter to fans.

"We are already hard at work on several new games including an all-new NASCAR racing sim created by DMi for PlayStation 4, Xbox One, and PC that we expect to release in 2016," he explained.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

U.S. Penetrated North Korean Networks Years Ago

The U.S. National Security Agency began tapping into North Korean computer networks in 2010, an effort that ultimately helped provide evidence to persuade the Obama administration that Pyongyang was behind the cyber attack on Sony Pictures, the New York Times reported on Sunday.

Citing former U.S. and foreign officials and a National Security Agency document, the Times said the spy agency was able to penetrate North Korean systems with the help of South Korea and other U.S. allies after first tapping into Chinese networks that connect North Korea to the rest of the world.

The newspaper quoted officials as saying the program grew into an effort to place malware that could track many networks and computers used by hackers in North Korea.

Such activity ultimately proved crucial in persuading President Barack Obama to implicate the North Koreans in the Sony attack, the officials told the paper.

It was the first time the United States directly accused another country of a cyber attack of such magnitude on American soil.

Obama "had no doubt" in this case, a senior U.S. military official told the Times.

North Korea has described the accusation as "groundless slander."

Sony’s network was crippled by hackers in November as the company prepared to release "The Interview," a comedy about a fictional plot to assassinate North Korean leader Kim Jong Un. The attack was followed by online leaks of unreleased movies and emails that caused embarrassment to executives and Hollywood personalities.

U.S. officials could not immediately be reached for comment.

China Blocks VPN Services That Skirt Online Censorship

China is blocking VPN services that let users skirt online censorship of popular websites such as Google and Facebook amid a wider crackdown on online information, tech companies and specialists said Friday.

The virtual private network provider Golden Frog wrote on its blog that the controls have hit a wide swath of VPN services. The popular provider Astrill informed its users this week that its VPN protocols for Apple mobile devices to access services such as Gmail have been blocked.

The Chinese government blocks thousands of websites to prevent what it deems politically sensitive information from reaching Chinese users. Many foreigners in China as well as millions of Chinese depend on VPNs to connect to servers outside the country and access blocked information and Google-based business tools. VPNs encrypt and reroute Internet traffic so that censors can’t tell what’s being accessed.

"The Chinese government has attempted to curtail the use of VPNs that its citizens use to escape the Great Firewall for a couple years," wrote Golden Frog President Sunday Yokubaitis in a statement. "This week’s attack on VPNs that affected us and other VPN providers is more sophisticated than what we’ve seen in the past."

The Chinese government’s agency for regulating the Internet did not immediately respond to questions.

China-based entrepreneur Richard Robinson said the controls have particularly hurt small- and medium-sized foreign companies that depend on VPNs. Many larger companies can afford direct connections to servers outside the country, he said.

Over the past weeks, Chinese censors have already blocked what remaining access there is to Gmail and other Google products. Google services have been periodically blocked or limited since 2010 when the company said it would no longer cooperate with China’s censors.

"These smaller businesses, they’re dependent on Gmail," Robinson said.

The crackdown comes during sensitive political times, as President Xi Jinping’s government prosecutes top officials accused of corruption, said Xiao Qiang, an adjunct professor with UC Berkeley’s School of Information.

"We all know that China is in the middle of a very ferocious power struggle or political cleansing under the name of an anti-corruption campaign," Xiao said. "That to me is a very clearly related fact with the amount of political rumors and information related to China’s high politics showing up in websites outside of China."

And while the controls hurt businesses that depend on online information and tools, Chinese censors are more worried about restricting political information, Xiao said.

Republican Net Neutrality Bill Allows ’Reasonable’ Network Management

Draft Net neutrality legislation released by Republican leaders in the U.S. Congress would prohibit broadband providers from blocking or selectively slowing legal Web content, but it would allow them to engage in "reasonable" network management.

The proposal would give broadband providers wide latitude to engage in network management, with a management practice deemed reasonable "if it is appropriate and tailored to achieving a legitimate network management purpose."

The draft legislation would also prohibit the U.S. Federal Communications Commission from reclassifying broadband as a regulated public utility, and it would stop the agency from creating any new Net neutrality rules.

The draft legislation is a "thoughtful path forward" that protects consumers online, said Representative Fred Upton, a Michigan Republican. "By clearly outlining the appropriate rules of the road, and leaving 20th century utility regulation behind, we can be sure that innovators continue full throttle in bringing remarkable new technologies to all Americans," Upton said in a statement. "This is the right solution that everyone, if they are serious in standing up for consumers, should be able to get behind."

Under the proposal’s network management definition, broadband providers can take into account their "particular network architecture and any technology and operational limitations" when crafting network management practices, according to the text of the draft bill.

The entire definition of a reasonable network management practice, running about 45 words, is borrowed from the FCC’s 2010 Net neutrality rules that were later partially overturned by an appeals court. But many advocates of strong Net neutrality rules protested a proposal earlier this year from FCC Chairman Tom Wheeler that would have allowed broadband providers to engage in "commercially reasonable" network management, saying it would give providers a wide exemption to the rules.

The network management definition in the draft bill could be a "loophole" for broadband providers, said John Bergmayer, senior staff attorney at Public Knowledge, a digital rights group advocating for strong Net neutrality rules.

The Republican proposal prohibits broadband providers from blocking and selectively slowing Web content, applications and services, but that’s "subject to reasonable network management." The draft bill does prohibit broadband providers from entering into paid traffic prioritization deals with now allowance for reasonable network management, although the bill appears to allow middle-mile traffic deals, like ones Netflix has signed with major broadband providers, Bergmayer said.

The draft legislation’s prohibition of the FCC reclassifying broadband under Title II of the Telecommunications Act is the wrong approach, added Matt Wood, policy director at digital rights group Free Press. "This bill would legalize any and every other form of discrimination that the ISPs could dream up," he said by email. "It does that by stripping the FCC of rule-making authority and handcuffing the agency’s ability to adapt to new circumstances."

The draft proposal’s prohibition against a Net neutrality rule-making proceeding at the FCC may be the biggest of several problems, Bergmayer added. The proposal would require the FCC to act on Net neutrality complaints filed by consumers or companies, and it’s unclear whether the FCC could set precedent by acting on a complaint, he said.

If a consumer brings a complaint to the FCC and wins, "is that practice now considered illegal in general for everyone?" he said. "Or, every time something happens that you don’t like, are you back at square one?"

Still, Public Knowledge is heartened to see movement on Net neutrality issues from top congressional Republicans, many of whom opposed any Net neutrality rules in recent years, Bergmayer said. The draft bill comes from Upton, chairman of the House Energy and Commerce Committee, and Senator John Thune, a South Dakota Republican and chairman of the Senate Commerce, Science and Transportation Committee.

"This goes much further than anything we would have expected to see, particularly from congressional Republicans just a year ago," Bergmayer said. "It does show that there is some consensus that something has to be done to protect consumers."

Both committees have hearings on the draft bill scheduled for next Wednesday.

Lizard Squad’s DdoS Service Hacked, Buyers’ Details Revealed

Lizard Squad, the group that took down the Sony PlayStation and Microsoft Xbox networks over the Christmas period, has received a dose of its own medicine with the news that it has itself been hacked.

Security blogger Brian Krebs reports that Lizard Squad s own DDoS-for-hire website   Lizardstresser.su - has been compromised.

The site is home to the group s LizardStresser tool which relies on thousands of hacked home routers to launch DDoS attacks.

Krebs reports that the site has been "completely compromised" and the details of over 14,200 registered users of the DDoS-for-hire service are in the hands of authorities.

Given how a Lizard Squad spokesman recently claimed that part of the group s motivation for its recent attacks was the highlighting of poor security practices, it is ironic to note that its own database of users was not encrypted   usernames and passwords were apparently stored in plaintext which, in terms of poor security mistakes, is about as big as they come.

Krebs says that only a few hundred of the users registered with LizardStresser ever paid for the website-disabling service - handing over around $11,000 in bitcoins - but they must surely be quaking in their boots right now, knowing that law enforcement now has the information it needs to identify them.

That’s not the only problem for Lizard Squad.

Since the group took out the PlayStation and Xbox networks, three alleged members have been questioned by police for their part in the DDoS. (Group member ’Ryan’ previously said there were only three members of the Squad.)

First to be collared was 22-year-old Vincent Omari who was apprehended by the South East Regional Organised Crime Unit (SEROCU) on 31 December 2014.

The arrest happened not long after ’computer security analyst’ Omari had given an interview to Sky News on 27 December in which his voice sounded remarkably similar to that of an anonymous Lizard Squad member who spoke on BBC radio the day before.

A second suspected member of Lizard Squad was later detained in Finland. Julius Kivimäki, 17, was questioned by Finnish police amid claims that he was the Lizard Squad spokesman Ryan who also spoke to Sky News.

Since then SEROCU, working with the FBI, arrested an 18-year-old man in Southport, UK in connection with the Xbox and PlayStation attack.

The unnamed individual was detained under the Computer Misuse Act 1990. The man has been bailed until May.

Silk Road 2.0 Deputy Arrested After 6-month Attack on Tor

With the trial of alleged Silk Road mastermind Ross Ulbricht under way for a second week, Department of Homeland Security (DHS) agents have also now arrested the alleged deputy of the illegal drug bazaar’s reboot, Silk Road 2.0.

Brian Richard Farrell, 26, of Bellevue, Washington, was arrested last week and charged on Tuesday with conspiracy to distribute heroin, methamphetamine, and cocaine, according to a statement from the office of Acting US Attorney Annette L. Hayes, for the Western District of Washington.

Farrell allegedly went by the handle "DoctorClu" on Silk Road 2.0, which sprang up in November 2013 following the government’s seizure of the first Silk Road website.

Alleged kingpin of Silk Road 2.0, Blake Benthall, also known as "Defcon", was arrested in November 2014 in San Francisco.

According to the criminal complaint filed on Tuesday, Farrell told agents he was a "key assistant" in a small staff that helped Benthall run the enterprise’s day-to-day operations.

Those tasks included tending to the computer infrastructure and programming code underlying the website; the terms of service and commission rates imposed on vendors and customers of the website; and the "massive" profits generated from the illegal business.

The complaint alleges that Farrell was also involved in approving new staff and vendors, as well as organizing a denial of service (DoS) attack on a competitor.

According to an affidavit by Special Agent Michael Larson, DHS agents tracked Silk Road 2.0 activity to Farrell’s home in July 2014.

Agents then watched Farrell’s comings and goings and interviewed a roommate who said that Farrell received UPS, FedEx and postal packages daily.

Farrell’s roommate told agents that he opened one "suspicious" package addressed to Farrell and found it contained 107 Xanax pills.

The investigation led to a search of Farrell’s Bellevue home on 2 January 2015, during which agents seized computers, drug paraphernalia, silver bullion bars worth $3,900, and $35,000 in cash, Larson said.

The charge levied against Farrell on Tuesday carries a mandatory minimum prison term of 10 years and a maximum punishment of life in prison.

According to Larson’s search warrant, the Silk Road 2.0 investigation has been based on a six-month infiltration attack launched against Tor, the anonymizing service that kept Silk Road 2.0 users anonymous.

From January 2014 to July 2014, agents managed to get what Larson described as "reliable" IP addresses for Tor and for services hidden behind its layers, including Silk Road 2.0. That included its main marketplace URL, its vendor URL, and its forum URL.

Agents used this data to track down Silk Road 2.0’s servers, which resulted in the site’s takedown in November 2014.

The data was also used to identify another 17 black markets hidden on Tor. Larson didn’t give details on these other Tor-hidden markets.

According to the government, as of September 2014, before the Feds shuttered it, Silk Road 2.0 was doing quite well, ringing up sales of about $8 million per month with a user base of 150,000 active participants.

Barrett Brown Sentenced to 5 Years in Prison Just for ’Re-Sharing Link to Hacked Material’

Barrett Brown, a journalist formerly served as an unofficial spokesman for the hacktivist collective Anonymous, was sentenced Thursday to over five years in prison, after pleading guilty to federal charges of "transmitting a threat in interstate commerce," "for interfering with the execution of a search warrant," and to being "accessory after the fact in the unauthorized access to a protected computer."

After already having served over 2 years (31 months) in detention, Texas court in Dallas has sentenced Barrett Brown to 63 months in federal prison and also ordered him to pay a little more than $890,000 in restitution and fines related to the 2011 hack of Stratfor Global Intelligence.

Over a year ago, another federal judge sentenced Anonymous member Jeremy Hammond to 10 years in prison for making millions of emails from the servers of security firm Stratfor public. It s Hammond who said that Brown simply linked to the hacked data.

Brown was arrested in 2012 and nailed with 12 cyber crime charges, including a fraud charge for spreading around the hyperlink to an IRC (Internet Relay Chat) channel where Anonymous members were distributing stolen information from the hack, including credit card details.

According to the Department of Justice, sharing the hyperlink was a crime because "by transferring and posting the hyperlink, Brown caused the data to be made available to other persons online, without the knowledge and authorization of Stratfor and the card holders."

However, nearly all of those charges were later dropped and replaced with three more centered upon acting as an accessory to hacking charges, obstruction of justice and allegedly threatening an FBI agent in a video posted to YouTube. Brown’s 2012 arrest came just hours after he posted a YouTube video called "Why I’m Going to Destroy FBI Agent Robert Smith."

For count 1 in the case, he receives 48 months in prison.
For count 2, he receives 12 months in prison.
For count 3, he receives 3 months in prison.

He is also ordered to pay $890,000 in restitution.

Brown s supporters from across the web had been hoping he would be able to get off with his last 31 months of time he spend in federal prison for what they insist was "merely linking to hacked material". Instead he got more along with a little huge amount in fine.

In a sentencing statement, Brown described the Stratfor hack and the shared link as still central to the government’s motives in the case. "The fact that the government has still asked you to punish me for that link is proof, if any more were needed, that those of us who advocate against secrecy are to be pursued without regard for the rule of law, or even common decency," Brown told the judge.

After receiving the sentence, Brown was sarcastically upbeat and released the following statement:

Good news!

The US Government decided today that because I did such a good job investigating the cyber-industrial complex, they’re now going to send me to investigate the prison-industrial complex. For the next 35 months, I’ll be provided with free food, clothes, and housing as I seek to expose wrongdoing by Bureau of Prisons officials and staff and otherwise report on news and culture in the world’s greatest prison system. I want to thank the Department of Justice for having put so much time and energy into advocating on my behalf; rather than holding a grudge against me for the two years of work I put into bringing attention to a DOJ-linked campaign to harass and discredit journalists like Glenn Greenwald, the agency instead labored tirelessly to ensure that I received this very prestigious assignment.

Wish me luck!

Feds Pay Woman $134 K Over Fake Facebook Profile Used in Drug Case

The federal government has changed course in a drug investigation in which agents pulled a woman s photos from her cell phone without her permission and used them to create a fake Facebook account that sought to trap drug dealers.

When Sondra Arquiett of New York sued over the incident last year, the Drug Enforcement Agency first claimed that she had granted implicit consent to use the photos, but now the government will instead pay Arquiett $134,000 to make the case go away.

The case first surfaced last year when BuzzFeed discovered court filings that described how, in 2010, law enforcement agents arrested Arquiett on drug charges and then surreptitiously took racy photos from her phone, including one showing her sitting astride a BMW in small shorts.

The DEA then created a Facebook profile purporting to be Arquiett and used it to contact at least one member of a drug ring. Arquiett only discovered the account when another friend asked her about it.

In her lawsuit, Arquiett sought $750,000, claiming invasion of privacy, violation of her constitutional rights and emotional distress.

The federal government s decision to settle the case was likely wise in light of increased attention paid by the Supreme Court and activists to privacy violations involving cell phones and social media.

According to the AP, which reported the settlement, the Arquiett deal does not specifically preclude the DEA from using such tactics in the future; however, a spokesperson did say the Justice Department was meeting with law enforcement to make clear the necessity of protecting the privacy and safety of third parties in every aspect of our criminal investigations.

Facebook has also stated that it does not approve of law enforcement creating fake profiles.

How Verizon and Turn Defeat Browser Privacy Protections

Verizon advertising partner Turn has been caught using Verizon Wireless’s UIDH tracking header to resurrect deleted tracking cookies and share them with dozens of major websites and ad networks, forming a vast web of non-consensual online tracking. Explosive research from Stanford security expert Jonathan Mayer shows that, as we warned in November, Verizon’s UIDH header is being used as an undeletable perma-cookie that makes it impossible for customers to meaningfully control their online privacy.

Mayer’s research, described in ProPublica, shows that advertising network and Verizon partner Turn is using the UIDH header value to re-identify and re-cookie users who have taken careful steps to clear their cookies for privacy purposes. This contradicts standard browser privacy controls, users’ expectations, and Verizon’s own claims that the UIDH header won’t be used to track users because it changes periodically.

This spectacular violation of Verizon users’ privacy made all the worse because of Verizon’s failure to allow even an opt-out has already had far-reaching consequences. Through Turn’s cookie syncing program (described below) the re-identification affects dozens of other sites and ad networks. According to Mayer’s research, many ad networks and high profile sites, including Facebook, Twitter, Yahoo, BlueKai, AppNexus, Walmart and WebMD, receive copies of the respawned cookie.Mayer identified a spectrum of blatancy by which the information was transmitted, from Referrer headers, through URL parameters, to literal replication of the Turn cookie by the other third party tracker. All of the companies we list do more than receive a Referrer, though a Referrer is enough to defeat the user’s attempt to delete cookies. We have replicated and expanded on some of Mayer’s results; in particular we observed Facebook and Twitter getting the Turn cookie through explicit cookie-syncing APIs. At this point, Mayer has observed Google receiving the respawned cookie via Referrer headers and is therefore very likely to have logged it, but we have not yet observed it being sent to DoubleClick’s Cookie Matching API. If these sites follow what we understand to be typical cookie syncing practices, they would also be circumventing cookie deletion. It is possible that some of these companies are unknowingly in violation of their own privacy policies and regulatory settlements as a result of Verizon and Turn’s practices.

This ongoing privacy fiasco reinforces how dangerous it is for ISPs to use their network control to impose non-standard new tracking methods on their customers.

Previously, EFF analyzed Verizon’s PrecisionID program, thanks to a suggestion from a concerned member. We found that Verizon reaches into their mobile customers’ web browsing requests as they pass through the Verizon network and tampers with them to insert a header that uniquely identifies each Verizon subscriber. Ad networks can use the header to access extended targeting data on all Verizon customers, such as address, age, sex, and interests. Verizon claims to offer an opt-out, but opting out does not actually remove the header. Instead, Verizon claims it will not share a customer’s demographic data after opt-out. But that means that third parties can and indeed are still using the Verizon header value as a unique tracking identifier that Verizon customers are powerless to change or delete, even after the user has "opted out" of the Verizon program. Nor does enabling the Do Not Track browser setting have any effect. In fact, Turn has told EFF that they do not believe that either Do Not Track or a user deleting their cookies is a signal that the user wishes to opt out from tracking. Turn ignores and circumvents these mechanisms, and uses the DAA’s pretend opt-out instead.

[Verizon’s] ongoing privacy fiasco reinforces how dangerous it is for ISPs to use their network control to impose non-standard new tracking methods on their customers.

EFF warned that third parties would use this undeletable header to circumvent browser privacy protections like cookie deletion and private browsing mode in a way not possible without the header. The Turn network is doing exactly that. Like most ad networks, Turn assigns their own unique cookie (called ’uid’) to everyone who visits any site that includes Turn’s tracking URLs. For other networks, deleting cookies from your browser effectively dissociates you with the reading history they have collected on you. However, Turn is more invasive: If you delete cookies, Turn will re-assign you the exact same ’uid’ cookie you just deleted.

Turn can only do this because Verizon sends the same unique UIDH header, so Turn can simply look up the UIDH value in an internal database. Because Verizon does not honor their customers’ opt-out by removing the UIDH header, Turn performs this cookie resurrection even for people who have opted out on Verizon’s site.

Turn also engages in cookie syncing, a widespread but sneaky workaround to the Web’s cookie security policies. Normally, your browser only sends Turn’s ’uid’ cookie back to Turn’s own servers. But when your browser visits a web page with Turn’s embedded tracking URLs, those URLs can load an additional tracker from another network, for instance Facebook. Facebook would then receive a request that includes both Turn’s uid and Facebook’s own cookies identifying an individual. Facebook records the relationship between identities, perhaps so they can accumulate data about individuals with help from with Turn. Cookie syncing becomes even more of a problem when one network uses illegitimate re-identification techniques on an individual, because, as Mayer’s research demonstrates, Turn’s resurrected cookie rapidly infects other ad networks, informing those networks about Internet reading or browsing history the individual asked them to forget. We call on all ad networks to suspend cookie syncing with Turn until they have fixed this issue, and to delete existing Turn cookie syncing data collected in violation of users’ privacy.

Turn’s activities are simply the easiest to observe, and the most egregious, since they are a Verizon partner. There are almost certainly other advertisers using the same technique, both within Verizon’s partner network and without. We’ve observed that Twitter and at least one other ad network have used UIDH. Mayer provides details on how he spotted Turn’s obvious re-identification, but ad networks can abuse UIDH in less obvious ways. For instance, they can assign cookies that are not identical to deleted ones, but are connected to the deleted cookies through a private database.

As we noted when we first wrote about this issue, the only way for Verizon customers to protect themselves against their ISP’s tampering is to install a VPN, an expensive and difficult option, especially on a mobile phone. Some people may also want to install a privacy-protecting browser extension, like Privacy Badger, Disconnect, or AdBlock Plus with the EasyPrivacy list. These extensions cannot protect against the UIDH header, but they may prevent ad network cookies from being sent, which can inhibit re-identification and cookie syncing.

Amidst the outrage following our November article, AT&T, who was also beginning a tracking header program, chose to abandon it. We call on Verizon to do the same

It is clear that Verizon does not understand the privacy risks it is imposing on its customers. They ignored their customers’ Do Not Track opt out requests. The UIDH program should be shut down today. Going forward, the company should undertake to obtain genuine prior, informed consent for any future tracking activities.

Update: Turn announced they will suspend their zombie cookie program by early February, but left open the possibility to resume in the future. We ask that they end the program permanently.

Big Brother: Can Your School Require Your Facebook Password?

The conversations around data privacy and internet safety just got hotter.

A new Illinois state law can now compel students to hand over their social media login credentials to their school if school and state officials believe it can help prevent hostile online behavior   raising privacy concerns among parents and students alike.

The law, which then-Governor Pat Quinn signed in August and went into effect Jan. 1, is an effort to curb cyberbullying and online harassment both in and out of the classroom, before it gets out of hand. Previously, Illinois schools could intervene if online bullying occurred during class hours.

Children need to understand that whether they bully a classmate in school or outside of school using digital devices, their actions have consequences, State Rep. Laura Fine (D-Glenview) said in a statement. Students should not be able to get away with intimidating fellow classmates outside of school.

On the other hand, as Illinois mom Sara Bozarth told local Fox affiliate KTVI: It s one thing for me to take my child s social media account and open it up, or for the teacher to look or even a child to pull up their social media account, but to have to hand over your password and personal information is not acceptable to me.

The discussion in Illinois mirrors similar conversations about cyberbullying and data privacy in the United States, as cities and counties across the country struggle to find ways to protect children online.

In 2013, a school district in Los Angeles was met with suspicion and media scrutiny when it spent more than $40,000 to monitor the social media profiles of its students for any signs of bullying or self-harm, the Los Angeles Times reported. In Denver last year, the Colorado Defense Bar opposed the passage of a cyberbullying bill that criminalized using social media to cause serious emotional distress on a minor.

Lawmakers in Albany County, New York also had to pare down their original bill against cyberbullying after the state Supreme Court, citing First Amendment rights, struck it down in July. And a software program in Washington County, Maryland that allows school officials to monitor students profiles for illegal and violent activity on and off campus, much to the chagrin of privacy advocates.

There s no doubt that cyberbullying can get bad. While definitions vary, cyberbullying is at its core online harassment   any aggressive behavior, insults, denigration, impersonation, exclusion, and activities related to hacking against a person or persons   done repeatedly over a period of time, according to the Pew Research Center. Figures vary regarding the prevalence of cyberbullying among children and young adults, but most research estimates that anywhere between 6 to 30 percent of teens have experienced some form of it.

The worst consequences are death and self-harm, as in the 2013 case of 12-year-old Rebecca Ann Sedwick, who committed suicide after a group of middle-school students barraged her with text messages urging her to kill herself.

 Every student should feel safe from harassment, whether that s in the school hallways or when using the internet or a cell phone, former Gov. Quinn said after he signed the bill in Illinois. In our technology-driven age, bullying can happen anywhere. This new law will help put an end to it.

But others argue that there are ways to protect children besides monitoring and surveillance.

Jim Steyer, CEO of nonprofit Common Sense Media, told NPR in 2013 that his company tries to focus on informing and educating kids from a young age instead of watching their every move. The company developed a curriculum on digital literacy and citizenship, Steyer said, which teaches students how to use digital technology safely and responsibly.

"Our approach is teaching kids empathy," he said. "I think that’s much better than spying on kids."

Windows 10: What You Missed at the Microsoft Event

Microsoft wasn’t kidding when it billed its Windows 10 event as the "next chapter" for the software company.

From hardware to holograms, the company packed a slew of announcements into a feature-packed presentation that lasted around 2 hours and 15 minutes.

Here’s a cheat sheet to Windows 10 and everything else that was announced at Microsoft’s Redmond, Washington, headquarters.

Let’s get right down to it. Windows 10, the operating system update that is so radical it prompted Microsoft to skip straight from Windows 8, will be coming to users "later this year."

While the vague release date may illicit a few groans from weary Windows 8 users, there is a spot of good news. The update will be free for users who have Windows 8.1, Windows 7 and Windows Phone 8.1.

"The free upgrade is primarily for developers to get everyone on one platform," Patrick Moorhead, an analyst at Moor Insights & Strategy, told ABC News. "It benefits Microsoft, too, as Windows 10 is a giant door to their services like One Drive and Office 365."

The world met Windows 10 at an event last year, however today Microsoft showed off new consumer driven features that support the company’s goal to increase productivity.

With Windows 10, you can stream Xbox One games to any PC or tablet in your house. You’re no longer married to the gaming console.

Better yet, two friends can even play a multi-player game with one person on Xbox and another on their PC.

Microsoft’s sassy virtual personal assistant, Cortana, will be integrated into Windows 10, where users can ask her to do things, such as pull up a certain PowerPoint presentation.

Proving that she’s becoming more like Samantha, the sultry virtual personal assistant in the movie "Her," Cortana can also take notes on your habits and tailor your experience. (Users control the notebook, so you can make sure Cortana only learns as much as you want her to.)

Microsoft unveiled a new browser today, called Project Spartan, but don’t think of it as a total Internet Explorer killer.

Moorhead said the faster, sleeker browser was developed to work best on more modern websites, however some businesses will still rely on Internet Explorer for compatibility.

Project Spartan comes with some exciting features, including the ability to write anywhere on a window and quickly share it.

For those who have a love-hate relationship with Internet Explorer, the news is welcome, but don’t expect to see the new browser anytime soon. Microsoft executives said it will not be in the first build of Windows 10.

The Microsoft Surface Hub is a new product category for the company as it takes on the challenge of bolstering workplace productivity.

While it looks like a white board, the device is an 84-inch, 4K display with a computer, built-in sensors, cameras, speakers, microphones to support workplace collaboration.

As Microsoft executive Hayete Gallot put it: "It’s got it all."

The same week Google Glass announced it was ending its Explorer program, Microsoft today unveiled an impressive new product that takes virtual eyewear to the next level using holograms.

While it’s unclear when HoloLens will be released, there was plenty to geek out over from Microsoft’s demo.

Imagine holographic Skype calls, turning your living room into a surreal gaming environment or designing a new product virtually.

Your digital and physical lives are now blended with HoloLens. The question is: While the technology is cool, will people actually want to spend money on the futuristic goggles?

Google Glass Will Be Back With a Vengeance

I tried on a pair of Google Glass for approximately five minutes about a year ago. I felt like an idiot. I looked like an idiot.

But I knew that at some point in the next three to five years, there would an iteration of Glass (or something from a competitor) that would feel as natural as wearing a pair of Ray-Bans. Or even better (or worse depending on your perspective), Google Glass would become something that slides into your eye like a contact lense. It’s hard to argue that something like that isn’t coming, it’s just a matter of when.

This week marked the end of an experiment for Google, and as of yesterday, the first version of Google Glass is no longer available for purchase. The move will naturally be fodder for tech pundits and contrarians who will make declarations about its success or failure. Some will call it a great triumph, others will call it a gigantic misfire. I think the verdict falls somewhere in the middle. But what about the future?

From a consumer standpoint, Google Glass was a PR mess, from idiots who refused to remove them in restaurants, using freedom of speech or expression as a crutch, to the simple fact that just being around someone wearing them made you feel as if you were under a creeper microscope. It was nearly impossible to accept any benefits of such a device, simply because the mere appearance of it was so polarizing.

However, Google Glass proved to be a much more worthy tool in specialized industries such as medicine, where doctors used it during surgical procedures. It’s also been a hit in warehouse environments, dramatically improving how workers can access information while keeping both hands free, which will probably get your package to you faster one day, if it hasn’t already.

Those use cases may not be sexy, but they are a reminder that while consumer technology is what drives conversation on tech blogs and social media, it’s not the ultimate definer of technical innovation.

That said, we’re still getting a new and hopefully improved design of Google Glass when the consumer edition arrives, and I’m excited and a little terrified of what the next few iterations will look like. These feelings have only intensified after watching a show like Black Mirror, which features a Google Glass-esque retinal implant that records everything you do from birth, allowing you to "review" and revisit any moment of your life.

Does that make you terrified about privacy? Don’t worry, Black Mirror has us covered there, too. The holiday special "White Christmas" featured technology that basically takes the act of blocking someone to a whole new, hilariously depressing level. Sure, we had the smoldering presence of Jon Hamm to soften the blow, but if you think this technology won’t ever become a reality in some form, you’re kidding yourself.

It remains to be seen if the future version of Google Glass will be surgically infused, or if human blocking will be one of its features, but as wearable technology becomes more present and intrusive in everyday life, the measures to counteract that intrusiveness will be just as bizarre.

This List Of 2014 s Worst Passwords, Including 123456, Is Embarrassing

The year of 2014, in many respects, was all about digital security. It wasn t just tech pundits or early adopters who were victimized Snapchat, Target, and Sony Entertainment all showed us that no one is immune. And don t get me started on the NSA. It s our responsibility as internet explorers to protect ourselves.

But according to SplashData s yearly list of the worst passwords on the internet (as compiled by more than 3 million leaked passwords from 2014), we are kind of lazy about the whole digital security thing. At least when it comes to properly locking the gates with a strong password.

Seriously.

Just take a look at the full list:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Last year, password topped the list so I guess we can find some small progress in the fact that most people are literally just typing integers as their passwords as opposed to robotically typing in literally the worst password you could ever use. Heck, we re even using dragon, a symbol of strength and fiery vengeance that is, sadly, also a horrible password.

There are easy ways to handle the problem of passwords. And the blame is not entirely on you   the whole password system is flawed and messy. But there are easy steps you can take to be more secure. One is using password management software to ensure that your passwords are strong enough, updated, and securely locked down and in a place you can find them.

For folks who can t be bothered to take that step, you can still do more. Even if your password isn t entirely random and disconnected from you personally (which is best), you can still choose your same obvious passwords and spruce them up a bit.

You can use the placement of keys on a keyboard to do this   for example, folks who use 123456 or qwerty can simply jumble those together based on the keys, making something like q1w2e3r4t5’. Want to make it easier? Take something you ll remember: My uncle lives in Kansas and make it your password MyUncleLivesInKansas and add his street address: MyUncleLivesInKansas207. These long, complex passwords are actually quite difficult to hack and are easy to remember. While these won t stop great hackers from getting into your stuff, at least you ll be taking steps to get out of the top ten.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.